



Healthcare Cybersecurity Solutions for Patient Safety

Cybersecurity to improve patient safety

www.arancia.io



Speak to an Expert
inquiry@arancia.ca

Scan the QR Code
to learn more about our
products and offerings.



Why the Connected Healthcare Landscape is a Target for Cybercriminals

Arancia's cybersecurity team has been supporting the healthcare sector for over a decade, giving us a deep understanding of the risks to patient safety posed by adversaries targeting healthcare technology platforms.

Cybercriminals target the healthcare ecosystem for many reasons, and over the next three years, attacks are expected to become more sophisticated as adversaries leverage AI-powered tools to execute double-extortion attacks which can encrypt files and also steal data at the same time.



Personal Health Information (PHI) & Research Data

Healthcare organizations store vast amounts of sensitive data, including personal health records (PHRs), medical histories, research data, clinical trials, insurance information, PII/PHI and other sensitive information. This data is valuable to cybercriminals because it can be sold on the dark web or used for identity theft, fraud, or blackmail.



Ransomware Attacks

Healthcare systems are complex in nature with Cloud assets, Electronic Medical Records (EMRs) integration with many on-prem systems, along with biomedical IoT and research networks. The compromise of one system could result in a lengthy downtime resulting in a patient safety issue. Organizations who are unprepared may have no other choice but to pay a large ransom.



Cyber Talent Shortage

Many healthcare delivery organizations simply cannot afford to attract or retain experienced and seasoned cyber professionals. This leads to cyber solutions being incompletely implemented or not monitored and maintained appropriately. This allows adversaries an opportunity to leverage these weaknesses to launch their attack.

Cyber Threat Landscape in Healthcare: Background

Rapid technological advancements have significantly transformed the cyber threat landscape in the healthcare sector. The World Health Organization (WHO) has highlighted those innovations in artificial intelligence, cyberattacks, and genetic engineering could pose severe risks to global biosecurity. A 2024 WHO report identified several ways in which cyber threats could impact healthcare, including unauthorized access to sensitive data or research, disruption of laboratory security systems, theft or sabotage of critical information, and espionage for competitive or malicious purposes. Additionally, cyberattacks could disable essential laboratory systems, disrupt operations, and compromise data integrity, leading to delays in critical research and jeopardizing safety protocols.

64% of healthcare providers faced at least one security breach since 2023.



200+ adversaries are actively targeting healthcare tracked by leading cyber intelligence firms.

84% of cloud-focused intrusions are linked to e-crimes.



75% increase in cloud environment intrusions in 2024.



Important Considerations



Advanced phishing attacks

Use impersonation tactics, deepfakes, vishing to compromise user identities to enable access to networks and systems.



Regulatory Complexity

Organizations must align with NIST CSF, HITRUST, PHIPA, SOC 2, HIPAA, ISO 27001, and other evolving security frameworks.



Digital Transformation Challenges

Virtual care, BYOD, and remote patient monitoring and expanded patient access challenge traditional security control methods.



Rising Privacy & Compliance Demands

Stricter regulations and evolving cyber insurance requirements make it harder for organizations to meet security obligations.

The following healthcare sectors are being targeted by both Nation-state and financially motivated cybercriminals.

- ▶ Bio Medical Companies
- ▶ Health Tech Organizations
- ▶ Hospitals and Clinics
- ▶ Pharmaceuticals

Nation States and Cybercriminal Actors are executing attacks across multiple assets simultaneously. These actors are executing attacks on the following types of assets:

- ▶ Desktop and Endpoints
- ▶ Medical Devices, Biomedical and Research Network
- ▶ Data Infrastructure & Network services
- ▶ Cloud Servers and Containers
- ▶ Network (ICS/SCADA/PLC)
- ▶ Identity and Active Directory

Staying ahead of Cybercriminals

Know Your Weakness before an Adversary does

It's important to know what your exposures are based on current attack scenarios so these risks can be mitigated before they are leveraged by attackers. Professional services such as those listed below can help improve your cyber readiness.

- ▶ Red Team Exercise
- ▶ Ransomware simulation & Compromise Assessments
- ▶ Threat Modeling Assessment
- ▶ Cloud Security Assessments
- ▶ Firewall and Active Directory (AD) Security Audits
- ▶ Table-Top Exercise to validate Cyber Incident & Breach Response Plan
- ▶ Implement Incident Response Retainers

Advance Security Monitoring with Automated Response

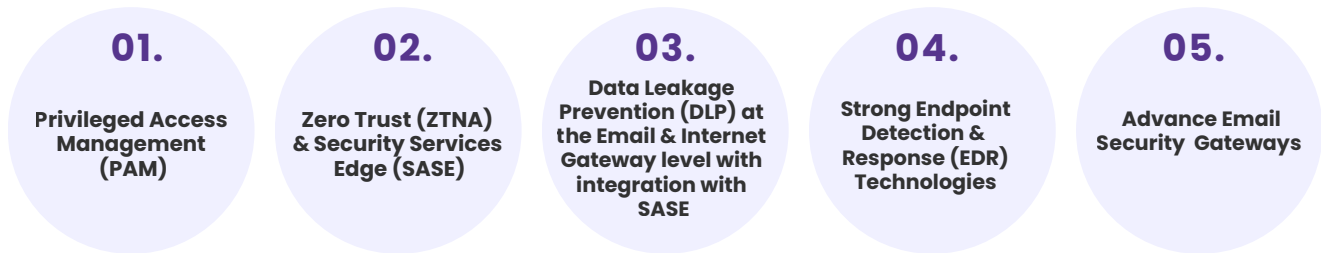
Traditional SIEM, MDR, XDR and other SOC Managed Services require a tremendous amount of effort to implement use cases that detect Adversarial behaviors and then raise alerts. It's important to have partners who provide a service for Threat Hunting along with a AI Powered Advance Security Platform.

Set a good foundation (Practical Advice)

Ensure your organization has implemented the basic system hardening & critical controls effectively. Establish a program to close vulnerabilities and gaps. Build a strong foundation of controls and have basic security hygiene in place. Arancia can provide assistance and operational support to manage these control areas if required.

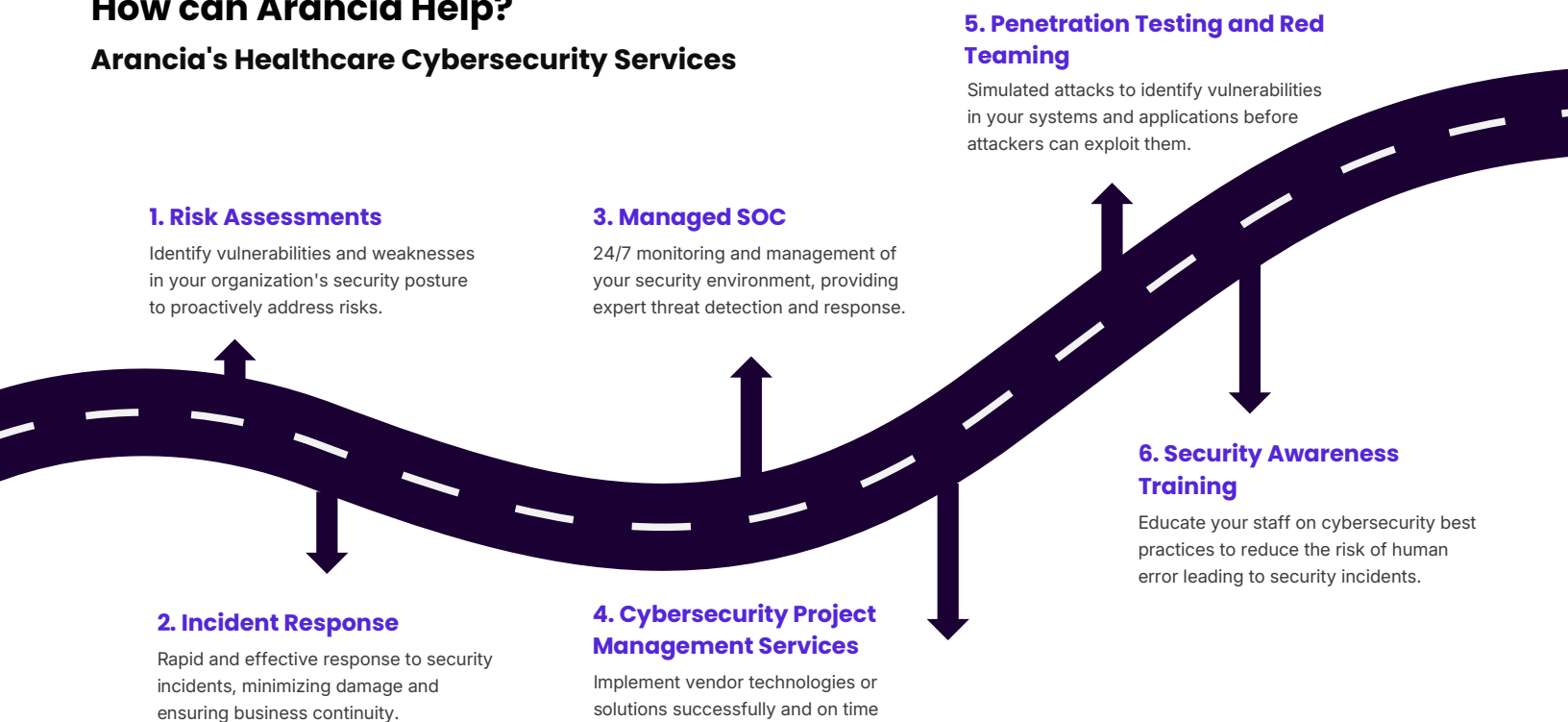
Key Cybersecurity Technology Enablement

It is important to review current cyber investments and implement key capabilities. Arancia has partnered with the leading vendors in the following control areas:



How can Arancia Help?

Arancia's Healthcare Cybersecurity Services



Benefits



Enhanced Security Posture

Proactively identify and address risks, strengthening your defenses against cyberattacks.



Compliance with Regulations

Ensure compliance with industry regulations and avoid costly penalties.



Reduced Downtime

Minimize disruptions to operations caused by security incidents, ensuring continuity of care.



Improved Patient Trust

Demonstrate your commitment to protecting patient data, building trust and confidence.